UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/669,784	09/24/2003	James C. Farmer	10002762-3	6401

22879 7590 12/02/2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
TSAI, SHENG JEN	
ART UNIT	**PAPER NUMBER**
2186	

NOTIFICATION DATE	DELIVERY MODE
12/02/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/669,784
Filing Date: September 24, 2003
Appellant(s): FARMER ET AL.

John P. Wagner, Jr.
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/02/2009 appealing from the Office action mailed 2/19/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Mater

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal Identifies the ground of rejections and the associated claims under rejection to be reviewed on appeal.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US 6,151,689	Garcia et al.	11-21-2000
US 5,915,025	Taguchi et al.	06-22-1999

US 4,255,811 Adler 03-10-1981

(9) Grounds of Rejection

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

>>> Claims 1,3-5, 15-16 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Garcia et al. (US 6,151,689, hereinafter referred to as Garcia), and in view of Taguchi et al. (US 5,915,025, hereinafter referred to as Taguchi).

It is noted that, in the following claim analysis, those elements recited by the claims are presented using **bold** font.

As to claim 1, Garcia discloses **a method for protecting memory space in a target storage device during a write operation in a computer system** [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)], **the method comprising**:

creating a single data packet [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, data and CRC; HADC packet, figure 3A,

including Header, Address, data and CRC in a single packet], **including user data** [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, data and CRC] **that is to be written in a write operation to said target storage device** [figure 6, 24b is the target storage device] **and key data** [for example, the CRC may be the corresponding key data; Accesses to the memory 28 are validated by the AVT logic 90 of each interface unit 24 (FIG. 5), using all of six checks: (1) that the CRC of the message packet carrying the request is error free, ..." (column 31, lines 10-25)] **that is used to establish authorization to store said user data** [Use of CRC in this manner operates to protect message packets from end to end because the router elements do not modify or regenerate the CRC as the message packet passes through. The CRC of each message packet is checked at each router crossing. A command symbol--"This packet Good" (TPG) or "This Packet Bad" (TPB)--is appended to every packet (column 5, lines 39-45); Garcia further teaches "access validation" in details from column 30, lines 56 through column 37, lines15]; **said key data being generated based upon a destination address of said write operation** [this limitation is taught by Taguchi, see below] **and based on a portion of said user data** [the corresponding key data in Garcia's invention is the CRC data, which is generated using user data -- Accesses to the memory 28 are validated by the AVT logic 90 of each interface unit 24 (FIG. 5), using all of six checks: (1) that the CRC of the message packet carrying the request is error free, ..." (column 31, lines 10-25); Use of CRC in this manner operates to protect message packets from end to end because the router elements do not modify or regenerate the CRC as the message

packet passes through. The CRC of each message packet is checked at each router crossing. A command symbol--"This packet Good" (TPG) or "This Packet Bad" (TPB)--is appended to every packet (column 5, lines 39-45); Garcia further teaches "access validation" in details from column 30, lines 56 through column 37, lines15; Taguchi also teaches generating key data using user data -- encryption key generation means for generating an encryption key depending on an attribute of data including instructions to be encrypted; decryption key generation means for generating a decryption key depending on an attribute of encrypted data (col. 26, lines 15-20)];

transmitting said single data packet to the target storage device [see figure 6];

determining whether said key data is valid [If the received message packet is found to have a bad CRC (or it is tagged with a "This Packet Bad" (TPB) command symbol, see below) the packet is discarded, and access is denied (column 31, lines 22-25)];

writing said user data into said target storage device only when said key data is valid [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)].

Regarding claim 1, Garcia teaches using CRC, which is generated from user data, as a key to establish authorization to store data, and does not teach that said key data being generated based upon a destination address of said write operation.

Taguchi teaches in the invention "Data Processing Apparatus with Software Protecting Functions" a mechanism for memory access protection [abstract] in which

the key data is generated based upon a destination address [figure 15 shows that the key to be used depends on the page number; figure 16 shows that the key to be used depends on the address tag; figure 17; A data processing apparatus with software protecting functions according to claim 1, wherein said encryption key generation means generates said encryption key depending on either an address or an address region of data to be encrypted; and wherein said decryption key generation means generates said decryption key depending on either said address or said address region of the encrypted data (col. 26, lines 36-44)] and based upon a portion of said user data [encryption key generation means for generating an encryption key depending on an attribute of data including instructions to be encrypted; decryption key generation means for generating a decryption key depending on an attribute of encrypted data (col. 26, lines 15-20)].

Taguchi also teaches that the motivation of using a key that is generated based on the destination address as well as user data is because it raises the level of protection, requires very little hardware storage, and can cover an unlimited number of memory areas [column 3, lines 56-62].

Therefore, it would have been obvious for one of ordinary skills in the art at the time of Applicants' invention to protect memory by using a key that is generated based on the destination address as well as user data, as demonstrated by Taguchi, and to incorporate it into the existing scheme disclosed by Garcia, because it offers the advantages of raising the level of protection, requiring very little hardware storage, and covering an unlimited number of memory areas.

As to claim 3, Garcia teaches that **the method of claim 1 further comprising: performing a Boolean operation on selected bits of said user data to generate said key data** [for example, the CRC may be the corresponding key data, which is calculated based on Boolean operations on Data bits].

As to claim 4, Garcia teaches that **the method of claim 1 further comprising**: **generating verification data from said user data at a controller of said target storage device** [Error-checking of the communication flow between the components of the processing system is achieved by adding a cyclic-redundancy-check (CRC) to the message packets that are sent between the elements of the system (column 5, lines 28-31)]; **and**

comparing said key data in said single data packet with said verification data to determine if said key data matches said verification data [The CRC of each message packet is checked not only at the destination of the message, but also while en route to the destination by each router element used to route the message packet from its source to the destination. If a message packet is found by a router element to have an incorrect CRC, the message packet is tagged as such, and reported to a maintenance diagnostic system (column 5, lines 31-40)].

As to claim 5, Garcia teaches that **the method of claim 4 further comprising: storing said user data to said target storage device if said key data matches said verification data** [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a

validation to read/write memory of that CPU, without which memory access is denied (abstract)].

As to claim 15, it recites substantially the same limitations as in claim 1, and is rejected for the same reasons set forth in the analysis of claim 1. Refer to "As to claim 1" presented earlier in this Office Action for details. Note that Taguchi teaches that said key data is generated based on a destination address as explained in "As to claim 1."

As to claim 16, it recites substantially the same limitations as in claim 5, and is rejected for the same reasons set forth in the analysis of claim 5. Refer to "As to claim 5" presented earlier in this Office Action for details.

As to claim 19, it recites substantially the same limitations as in claim 4, and is rejected for the same reasons set forth in the analysis of claim 4. Refer to "As to claim 4" presented earlier in this Office Action for details.

As to claim 20, it recites substantially the same limitations as in claim 4, and is rejected for the same reasons set forth in the analysis of claim 4. Refer to "As to claim 4" presented earlier in this Office Action for details. Also see figure 6 of Garcia et al.

>>> Claims 8-13, 15-16 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Garcia et al. (US 6,151,689, hereinafter referred to as Garcia), in view of Adler (US 4,255,811), and further in view of Taguchi et al. (US 5,915,025, hereinafter referred to as Taguchi).

As to claim 8, Garcia discloses **a system for conducting a protected memory write to a target storage device in a single transaction within a computer system** [CPUs and I/O devices may write to, or read from, memory of a CPU of the system.

Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract); figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, data and CRC], **the system comprising**:

Means for simultaneously delivering user data and key data to a controller of said storage device in a single data packet [HADC packet, figure 3A, including Header, Address, data and CRC in a single packet]**, wherein said user data is to be written to said storage device** [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, data and CRC; figure 6, 24b is the target storage device] **and key data** [for example, the CRC may be the corresponding key data; Accesses to the memory 28 are validated by the AVT logic 90 of each interface unit 24 (FIG. 5), using all of six checks: (1) that the CRC of the message packet carrying the request is error free, ..." (column 31, lines 10-25)] **is used to establish authorization to store said user data** [Use of CRC in this manner operates to protect message packets from end to end because the router elements do not modify or regenerate the CRC as the message packet passes through. The CRC of each message packet is checked at each router crossing. A command symbol--"This packet Good" (TPG) or "This Packet Bad" (TPB)--is appended to every packet (column 5, lines 39-45); Garcia further teaches "access validation" in details from column 30, lines 56 through column 37, lines15]; **said key data being generated based upon a system clock setting of said computer system** [this limitation is taught by Adler, see

below]; **based on a destination address of a write operation** [this limitation is taught by Taguchi, see below]; **and based on a portion of said user data** [the corresponding key data in Garcia's invention is the CRC data, which is generated using user data -- Accesses to the memory 28 are validated by the AVT logic 90 of each interface unit 24 (FIG. 5), using all of six checks: (1) that the CRC of the message packet carrying the request is error free, ..." (column 31, lines 10-25); Use of CRC in this manner operates to protect message packets from end to end because the router elements do not modify or regenerate the CRC as the message packet passes through. The CRC of each message packet is checked at each router crossing. A command symbol--"This packet Good" (TPG) or "This Packet Bad" (TPB)--is appended to every packet (column 5, lines 39-45); Garcia further teaches "access validation" in details from column 30, lines 56 through column 37, lines15]; **and**

Means for determining whether said key data authorizes writing said user data to said storage device [If the received message packet is found to have a bad CRC (or it is tagged with a "This Packet Bad" (TPB) command symbol, see below) the packet is discarded, and access is denied (column 31, lines 22-25); CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)].

Regarding claim 8, Garcia teaches using CRC, which is generated from user data, as a key to establish authorization to store data, and does not teach that said key data being generated based upon a system clock setting of said computer system.

Adler teaches in the invention "Key Controlled Block Cipher Cryptographic System" a mechanism for memory access protection in which a valid key is required to be granted access right to certain pages of a memory [All authorized subscribers who are permitted access to data within the network are assigned a unique key consisting of a combination of binary symbols. The central processing unit within the computing network contains a complete listing of all distributed authorized subscriber keys. All communications transmitted from terminal input are encrypted into a block cipher by use of the cryptographic system operating under the control of the subscriber key which is inputted to the terminal device. At the receiving station or central processing unit, an identical subscriber key which is obtained from internal tables stored within the computing system is used to decipher all received ciphered communications (abstract)].

Specifically, Adler teaches that a key is generated based on a system clock setting of said computer system [figure 4 shows "key generation clock" being used to generate keys; The second is the key generation clock K which controls the operation of the key generation shift registers shown in FIGS. 3A and 3B which sequentially generate the key material for each of the rounds (column 6, lines 7-11); column 6, lines 1-21].

Adler also teaches that the motivation of using a key that is generated based on a system clock setting of said computer system is because it allows generation of keys of great cryptographic strength by iterating the algorithm many more rounds than practically possible [column 14, lines 46-53].

Therefore, it would have been obvious for one of ordinary skills in the art at the time of Applicants' invention to protect memory by using a key that is generated based on a system clock setting of said computer system, as demonstrated by Adler, and to incorporate it into the existing scheme disclosed by Garcia, because it allows generation of keys of great cryptographic strength by iterating the algorithm many more rounds than practically possible.

Regarding claim 8, Garcia in view of Adler does not teach that said key data being generated based on a destination address of a write operation.

Taguchi teaches in the invention "Data Processing Apparatus with Software Protecting Functions" a mechanism for memory access protection [abstract] in which the key data is generated based upon a destination address [figure 15 shows that the key to be used depends on the page number; figure 16 shows that the key to be used depends on the address tag; figure 17; A data processing apparatus with software protecting functions according to claim 1, wherein said encryption key generation means generates said encryption key depending on either an address or an address region of data to be encrypted; and wherein said decryption key generation means generates said decryption key depending on either said address or said address region of the encrypted data (col. 26, lines 36-44)] and based upon a portion of said user data

[encryption key generation means for generating an encryption key depending on an attribute of data including instructions to be encrypted; decryption key generation means for generating a decryption key depending on an attribute of encrypted data (col. 26, lines 15-20)].

Taguchi also teaches that the motivation of using a key that is generated based on the destination address as well as user data is because it raises the level of protection, requires very little hardware storage, and can cover an unlimited number of memory areas [column 3, lines 56-62].

Therefore, it would have been obvious for one of ordinary skills in the art at the time of Applicants' invention to protect memory by using a key that is generated based on the destination address as well as user data, as demonstrated by Taguchi, and to incorporate it into the existing scheme disclosed by Garcia in view of Adler, because it offers the advantages of raising the level of protection, requiring very little hardware storage, and covering an unlimited number of memory areas.

As to claim 9, Garcia teaches that **the system of claim 8 further comprising: means for writing said user data to said target storage device only when said key data authorizes writing said user data** [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)].

As to claim 10, Garcia teaches that **the system of claim 8 further comprising:**

means, at an originating device, for calculating said key data using an algorithm before said user data and said key data is sent to said storage device [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, Data and CRC, and CRC is calculated using Data; If the received message packet is found to have a bad CRC (or it is tagged with a "This Packet Bad" (TPB) command symbol, see below) the packet is discarded, and access is denied (column 31, lines 22-25)].

As to claim 11, Garcia teaches that **the system of claim 10 wherein said algorithm calculates said key data from said user data** [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, Data and CRC, and CRC is calculated using Data].

As to claim 12, Garcia teaches that **the system of claim 8 further comprising**:

Means for generating verification data at said target storage device controller [Error-checking of the communication flow between the components of the processing system is achieved by adding a cyclic-redundancy-check (CRC) to the message packets that are sent between the elements of the system (column 5, lines 28-31)];

and

Means for comparing said verification data to said key data [The CRC of each message packet is checked not only at the destination of the message, but also while en route to the destination by each router element used to route the message packet from its source to the destination. If a message packet is found by a router element to have an incorrect CRC, the message packet is tagged as such, and reported to a maintenance diagnostic system (column 5, lines 31-40)].

As to claim 13, Garcia teaches that **the system of claim 8 wherein said determining means further comprising: means for authorizing writing of said user data only where said verification data matches said key data** [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)].

As to claim 15, it recites substantially the same limitations as in claim 8, and is rejected for the same reasons set forth in the analysis of claim 8. Refer to "As to claim 8" presented earlier in this Office Action for details. Note that Alder teaches that said key data is generated based on a system clock setting of said computer system as explained in "As to claim 8."

As to claim 16, it recites substantially the same limitations as in claim 5, and is rejected for the same reasons set forth in the analysis of claim 5. Refer to "As to claim 5" presented earlier in this Office Action for details.

As to claim 19, it recites substantially the same limitations as in claim 4, and is rejected for the same reasons set forth in the analysis of claim 4. Refer to "As to claim 4" presented earlier in this Office Action for details.

As to claim 20, it recites substantially the same limitations as in claim 4, and is rejected for the same reasons set forth in the analysis of claim 4. Refer to "As to claim 4" presented earlier in this Office Action for details. Also see figure 6 of Garcia et al.

(10) Response to Arguments

Appellants' arguments have been fully and carefully considered with Examiner's answers set forth below.

Answer to Argument 1. regarding Claims 1, 3-5, 15-16 and 19-20

(1) Appellants contend that neither Garcia nor Taguchi, alone or in combination teach or suggest the limitations recited in claim 1. Specifically, Appellants argue that the data in the packet of figures 3A-4C of the Garcia reference is "input/output data," and not "user data," as recited in the claims. The Examiner disagrees.

First, Garcia's invention is directed toward facilitating delivering user-oriented data efficiently and reliably over a communication network. For example, Garcia teaches [Computing systems, such as those described above, are often used for electronic commerce: electronic data interchange (EDI) and global messaging. Today's demands upon such electronic commerce, however, is demanding more and more throughput capacity as the number of users increases and messages become more complex. For example, text-only e-mail, the most widely used facility of the Internet, is growing significantly every year. The Internet is increasingly being used to deliver image, voice, and video files. Voice store-and-forward messaging is becoming ubiquitous, and desktop video conferencing and video-messaging are gaining acceptance in certain organizations. Each type of messaging demand successively more throughput (col. 3, line 66 to col. 4, line 11)].

Note that the above cited passage clearly states that the data of interest is user-oriented data such as text-only e-mail, image, voice and video files. It also particularly

point out that the goal is to provide enough throughput in order to meet the demands of a number of users. Therefore, the type of data disclosed in Garcia's invention focuses on "user data" as recited in the claims.

Second, figures 3A~3D and 4A~4C of Garcia show various types of packets, comprising Header, Address, data and CRC [HADC packet, figure 3A, including Header, Address, data and CRC in a single packet]. Note that the "data" packets specifically refers to "payload data," or "user data" as explained above, rather than the Header, Address or CRC, which are "overhead data" instead of "payload/user data."

Third, Garcia also teaches that [This allows the CPU 12 to manage write transfers into a user data structure or buffer area in the memory 28 ... (col. 34, lines 39-41)]. This is yet another piece of evidence that Garcia's invention is directed toward facilitating delivering user-oriented data.

Fourth, the term "input/output data" refers to the functional aspect of the data being inputted and outputted to and from the computer system. In other words, the user data is channeled through the input/output ports of the computer system for processing and transmission. Therefore, "user data" and "input/output data" merely refers to the different aspects of the same data objects -- "user data" refers to the nature/type of the data while "input/output data" refers to how the "user data" is to be processed, and they are certainly not mutually exclusive of each other.

Therefore, Garcia clearly teaches the limitation of "user data."

(2) Appellants also contend that, in Taguchi's invention, the key data is not sent in a single packet with the user data.

However, the limitation that a "single packet" containing both key data and user data is taught by the Garcia reference, as explained below:

First, Garcia explicitly teaches packets that contain both "user data" and "key data -- for example, figures 3A shows a HADC packet comprising Header, Address, data and CRC fields, where the "data" field represents "user data" (as explained in part (1) of this section), and the CRC is the corresponding "key data."

Note that the only limitation recited in claim 1 regarding the subject matter of "key data" is "to establish authorization to store said user data." With respect to this limitation, Garcia teaches [(column 5, lines 39-45) -- Use of CRC in this manner operates to protect message packets from end to end because the router elements do not modify or regenerate the CRC as the message packet passes through. The CRC of each message packet is checked at each router crossing. A command symbol--"This packet Good" (TPG) or "This Packet Bad" (TPB)--is appended to every packet; Garcia further teaches "access validation" in details from column 30, lines 56 through column 37, lines15, specifically, Garcia further teaches (column 31, lines 10-25) -- Accesses to the memory 28 are validated by the AVT logic 90 of each interface unit 24 (FIG. 5), using all of six checks: (1) that the CRC of the message packet carrying the request is error free, ..., The first check is made at the packet receiver 96 by the CRC logic checker 106, as discussed above. If the received message packet is found to have a bad CRC (or it is tagged with a "This Packet Bad" (TPB) command symbol, see below) the packet is discarded, and access is denied"].

Hence Garcia' invention uses CRC as a validation check to verify that the accessing to the memory is properly authorized with the correct/good CRC, and thus the CRC qualifiers as a "key data."

Second, the Taguchi reference is relied on only to teach the limitation that said key data being generated based upon a destination address of said write operation. It is noted that one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Thus, the limitation of "a single packet" is taught by Garcia in view of Taguchi because it is taught by the Garcia reference.

Answer to Argument 2. regarding Claims 8-13, 15-16 and 19-20

(1) Appellants contend that claims 8-13, 15-16 and 19-20 are patentable because Garcia in view of Taguchi fails to teach "a single data packet with user data," and neither does Adler.

However, Examiner has provided answer to address this argument in "**Answer to Argument 1.**" of this section that the Garcia reference alone teaches the limitation "a single data packet with user data." Refer to "**Answer to Argument 1.**" for details.

(11) Related Proceedings Appendix

There are no decisions rendered by a court or the Board that may directly affect, be affected by, or have a bearing on the decision of the Board in the instant appeal.

/Sheng-Jen Tsai/ Primary Examiner, Art Unit 2186
/Matt Kim/ Supervisory Patent Examiner, Art Unit 2186
/Kevin L Ellis/ Supervisory Patent Examiner, Art Unit 2117

November 24, 2009